REMARKS

Claims 1, 3-12, 14-32, 34, 38-41, 44-56, 58-62, 64-67, and 69-92 are pending in the application. Claims 1, 3-12, 14-32, 34, 38-41, 44-56, 58-62,6 4-67, and 69-92 stand rejected under 35 U.S.C. 103(a).

Claim Amendments

The foregoing amendment clarifies the expression of the invention. Support for the amendment is found throughout the specification and in the original claims as detailed below. Accordingly, no new matter has been added. Independent claims 1, 32, 41, and 81are amended to focus, for example, on the method and system for securely storing data for an owner including, for example, information relating to the owner's estate, such as an electronic copy of the owner's will, by entering the data on a virtual wallet application residing, for example, on one or both of the owner's personal computer and the server of a trusted third party, such as a bank. (Spec. p. 6, line 22-p. 7, line 5)

The virtual wallet application automatically assigns a primary aspect of a secret access device to the owner for accessing the data stored on the virtual wallet application, and a virtual executor functionality of the virtual wallet application is preprogrammed to escrow a secondary aspect of the secret access device for accessing the data stored on the virtual wallet application conditioned on the occurrence of an event, such as death or incompetence, that renders the owner incapable of acting on the owner's own behalf. (Spec. p. 6, lines 12-21; p. 8, line 26-p. 9, line 8) Upon receiving verification of the occurrence of the event by the virtual executor functionality via the trusted third party from a personal representative of the owner, the virtual executor functionality provides access to the stored data by the trusted third party on behalf of the owner's personal representative utilizing the secondary aspect of the secret access device. (Spec. p. 9, lines 9-23)

In addition, independent claims 56, 62, 67 and dependent claims 15-18, 21, 25-27, 44-47, 51-56, 58-62, 64-71, 74, 82, 83, and 96-92, the limitations of which are included in other claims, are canceled, and dependent claims 4, 7, 19, 20, 22, 23, 28, 38, 48, 49, 73, 75, 79, 84, and 85 are amended to correspond generally to the amendment of claims 1, 32, 41, and 81.

Claim Rejections - 35 USC § 103

Claims 1, 3-12, 14-32, 34, 38-41, 44-56, 58-62, 64-67, and 69-92 stand rejected stand rejected over Fischer (U.S. 6,141,423) in view of Rosen (U.S. 5,453,601) under 35 U.S.C. 103(a). The rejection is respectfully traversed and reconsideration is requested. The references asserted do not teach or suggest the claimed invention.

By way of background, an embodiment of applicant's claimed invention provides a system and method for securely storing, updating and managing the owner's electronic data relating to the owner's estate, such as an electronic copy of the owner's will, and accessing the stored data by a trusted third party, such as a bank, upon the occurrence of an event that renders the owner unavailable or incapable of action, such as the death or incompetence of the owner. The system for an embodiment of the present invention makes use of application software, such as a virtual wallet that resides, for example, on either or both of the owner's PC or the trusted third party's server. The virtual wallet application automatically assigns a primary aspect of a secret access device to the owner for accessing the data, and a virtual executor functionality of the virtual wallet application is preprogrammed to escrow a secondary aspect of the secret access device for accessing the data conditioned on the occurrence of the event, such as the owner's death or incompetence. Upon receiving verification of the occurrence of the event by the virtual executor functionality, the virtual executor functionality provides access to the stored data utilizing the secondary aspect of the secret access device.

These features, recited in independent claims 1, 32, 41, and 81, as well as additional features of the dependent claims, are believed to be clearly patentable over the applied prior art. The above-noted aspects are not disclosed or suggested by the references asserted against the claims of record. Specifically, the asserted references fail to provide key features of the invention, and the claimed invention is patentably distinct from the cited references.

Fischer discloses a mechanism in which a computer purchaser is prompted to enter password or other secret identification information, which is encrypted under the control of a public key of the computer vendor or manufacturer and stored in the computer as an escrow security record. (Col. 6, lines 26-45). If the computer owner forgets the password and furnishes documentary evidence to the vendor or manufacturer that matches the stored information, the vendor or manufacturer gives the owner the secret key. (Col. 6, lines 46-64). The Fischer patent neither teaches nor suggests the method and system for securely storing estate-related data for an owner as contemplated by applicant's claimed invention.

Rosen discloses a monetary system using money modules for generating issuing, distributing, accepting, storing and transferring electronic money using public/private key cryptography to secure information exchanged between two money modules. (Col. 14, lines 10-58). Neither does Fischer in view of the Rosen patent teach or suggest the method and system for securely storing estate-related data for an owner as contemplated by applicant's claimed invention.

The claimed combinations are not taught or suggested by Fischer or Rosen either separately or in combination with one another. Fischer discloses a mechanism for safekeeping, for example, password information for a computer purchaser by the computer vendor or manufacturer, in case the computer purchase loses or forgets the password, and Rosen discloses the well known use of public/private key cryptography to secure information. The above-noted aspects of applicant's claimed invention are not disclosed or suggested by Fischer or Rosen either separately or in any combination with one another.

Version With Markings to Show Changes Made

Amendments in the Claims:

In accordance with 37 CFR 1.121(c), the following versions of the claims as rewritten by the foregoing amendment show all the changes made relative to the previous versions of the claims.

1. (Twice Amended) A method for securely storing data for an owner, comprising:

storing the data for the owner consisting at least in part of information relating to the owner's estate by entering the data on a virtual wallet application for the owner, the virtual wallet application residing at least in part on a server of a trusted third party and having a virtual executor function;

automatically assigning a primary aspect of a secret access device for the virtual wallet application to the owner by the virtual wallet application for accessing the stored data;

automatically escrowing a secondary aspect of the secret access device for the virtual wallet application by the virtual executor function conditioned on the occurrence of an event that renders the owner incapable of acting on the owner's own behalf;

receiving verification of the occurrence of the event by the trusted third party from a personal representative of the owner upon the occurrence of the event; and

accessing the stored data by the trusted third party on behalf of the owner's personal representative with the escrowed secret access device.

4. (Amended) The method of claim 3, wherein entering the data further comprises entering the data by the owner at the terminal coupled to [a] the server.

Cancel claim 6, without prejudice.

7. (Amended) The method of claim [6] 4, wherein the trusted third party's server further comprises a financial institution server.

Cancel claims 15-18, without prejudice.

19. (Amended) The method of claim [17] 4, wherein entering the data further comprises entering the data on [a] the virtual wallet application residing at least in part on the terminal.

20. (Amended) The method of claim 1, wherein storing the data further comprises storing at least one category of information by [a] the virtual wallet application for the owner selected from a group of information consisting of identification information, authentication information, certificate information, access key information, PIN number information, credit card account information, debit card information, bank account information, and other personal information.

Cancel claim 21, without prejudice.

22. (Amended) The method of claim [21] 1, wherein automatically assigning the primary aspect of the secret access device further comprises automatically assigning the primary aspect of the secret access device to the owner at a terminal.

23. (Amended) The method of claim 22, wherein automatically assigning the primary aspect of the secret access device further comprises automatically assigning the primary aspect of the secret access device by the virtual wallet application residing at least in part on [a] the server coupled to the terminal.

Cancel claims 25-27, without prejudice.

28. (Amended) The method of claim 23, wherein automatically assigning the primary aspect of the secret access device further comprises automatically sending information about the secret access device to the owner at the terminal coupled to the server over a network.

32. (Twice Amended) A method for securely storing data for an owner, comprising:

storing the data for the owner consisting at least in part of an electronic copy of the owner's will on a virtual wallet application for the owner, the virtual wallet application residing at least in part on a server of a trusted third party and having a virtual executor function;

automatically assigning a secret device to the owner for accessing the stored data on the virtual wallet application, wherein automatically assigning the secret device further comprises automatically assigning the secret device by the virtual wallet application with at least two access aspects comprising an owner's access aspect and a trusted third party's access aspect;

automatically [storing] escrowing the trusted third party's access aspect by [a] the virtual executor [aspect] function of [a] the virtual wallet application for the owner[;

automatically escrowing the secret device] conditioned on the occurrence of an event comprising one of the owner's death and the owner's incompetence;

receiving verification of the occurrence of the event by the trusted third party from a personal representative of the owner upon the occurrence of the event; and

[accessing] providing access to the stored data by the trusted third party for the owner's personal representative with the trusted third party's access aspect of the escrowed secret device.

38. (Twice Amended) The method of claim 32, wherein automatically [storing] escrowing the trusted third party's access aspect further comprises automatically storing the trusted third party's access aspect by the virtual executor function of the virtual wallet application on [a] the server of the trusted third party.

41. (Twice Amended) A method for securely storing data for an owner, comprising:

storing the data for the owner consisting at least in part of information relating to the owner's estate on a virtual wallet application residing at least in part on a trusted third party's server and at least in part on the owner's personal computer coupled to the server;

automatically assigning a primary aspect of a secret device to the owner for accessing the stored data;

automatically escrowing a secondary aspect of the secret device by a virtual executor function of the virtual wallet application conditioned on the occurrence of an event consisting of one of the owner's death and the owner's incompetence[, wherein automatically escrowing the secret device further comprises automatically escrowing a trusted third-party's access aspect of the secret device by a virtual executor function of the virtual wallet application for the owner];

receiving verification of the occurrence of the event by the virtual executor function from a personal representative of the owner via the trusted third party; and

[accessing] providing access for the personal representative to the stored data with the escrowed secret device.

Cancel claims 44-47, without prejudice.

48. (Amended) The method of claim [47] 1, wherein automatically escrowing the secondary aspect of the secret access [information] device further comprises automatically storing at least one type of secret access information selected from a group of secret access information consisting of identification information, authentication information, certificate information, access key information, PIN number information, and password information.

49. (Amended) The method of claim 1, wherein automatically escrowing the secondary aspect of the secret access device further comprises automatically escrowing decryption infrastructure for the owner.

Cancel claims 51-56, without prejudice.

Cancel claims 58-62, without prejudice.

Cancel claims 64-71, without prejudice.

73. (Amended) The method of claim 72, wherein automatically updating the technology aspects further comprises automatically updating technology aspects of the data by a virtual archivist function of [a] the virtual wallet application.

Cancel claim 74, without prejudice.

75. (Amended) The method of claim [74] 73, wherein automatically updating the technology aspects further comprises automatically updating the technology aspects by the virtual archivist function of the virtual wallet application on the server of [a] the trusted third party.

79. (Amended) The method of claim 1, wherein storing the data further comprises receiving the data from another party by [a] the virtual wallet application for the owner.

81. (Twice Amended) A system for securely storing data for an owner, comprising:

[means for] a virtual wallet application residing at least in part on a server of a trusted third party and capable of storing the data consisting at least in part of information related to the owner's estate for the owner;

[means associated with the storing means] wherein the virtual wallet application is adapted for automatically assigning a primary aspect of a secret access device for the virtual wallet application to the owner for accessing the stored data;

[means associated with the storing means] a virtual executor function of the virtual wallet application preprogrammed for automatically escrowing a secondary aspect of the secret access device for the virtual wallet application conditioned upon the occurrence of an event comprising one of the owner's death and the owner's incompetence,[;

means associated with the storing means for] and upon receiving verification of the occurrence of the event via the trusted third party from a personal representative of the owner,[; and

means associated with the storing means] for [accessing] providing access to the stored data with the escrowed secondary aspect of the secret access device for the personal representative of the owner[, the means for storing the data further comprising a virtual wallet application having a virtual executor function].

Cancel claims 82 and 83, without prejudice.

84. (Amended) The system of claim [83] 81, [wherein the means for storing the data] further [comprises] comprising a terminal coupled to the server.

85. (Amended) The system of claim 84, [wherein the means for storing the data] further [comprises] comprising a network coupling the terminal to the server.

Cancel claims 86-92, without prejudice.

Conclusion

In view of the foregoing amendment and these remarks, each of the claims remaining in the application is in condition for immediate allowance. Accordingly, the examiner is requested to reconsider and withdraw the rejection and to pass the application to issue. The examiner is respectfully invited to telephone the undersigned at (336) 607-7318 to discuss any questions relating to the application.

Respectfully submitted,

John M. Harrington (Reg. No. 25,592)
for George T. Marcou (Reg. No. 33,014)

Kilpatrick Stockton LLP
607 14th Street, NW, Suite 900
Washington, DC 20005
(202) 508-5800

T0091-178714
WINLIB01:924773.1